

Management strategies of Bring Your Own Device

Peixuan Li and Liang Yang

School of Economics and Business Administration, Chongqing University, Chongqing, 400044, China

Corresponding Email: 357005895@qq.com

Abstract. The rapid development of mobile Internet and mobile terminals promote business office system from PC to mobile terminals gradually. Thus Bring Your Own Device (BYOD) has become one of the important development trends of enterprise office mode. We analyse the driving factors of implementing Bring Your Own Device, then point out some problems in the process of implementing Bring Your Own Device. Further, we propose the corresponding management strategies of Bring Your Own Device in order to provide references for enterprises to meet the need of mobile office.

Keywords. Bring your own device, management strategies, mobile internet.

1 Introduction

Internet and mobile communication are two major technology which grow rapidly and have great market potential today. Mobile Internet, the combination of them, is growing at an explosive speed and has brought great changes to various industries in recent years [1-2]. According to Cisco's 2016 global mobile data traffic forecast report release, the number of mobile users will reach 5.5 billion by 2020, accounting for 70 percent of the global population, and the number of smart mobile devices is expected to 72 percent of total global mobile devices, which is growing rapidly compared with 36 percent in 2015 [3]. This can be seen the advent of the era of mobile is unstoppable.

With the rapid development of mobile Internet and mobile intelligent terminals, employees' pursuit of new technology and personalization promotes enterprises' increasing demand for mobile applications, and enterprises' daily office work are gradually expanding from PC to mobile terminals. Bring Your Own Device (BYOD) as one of important mobile office modes has received the academia's extensive attention in recent years. At present, the literature mainly focus on BYOD's concept, development process, development status, demand level, the advantages and disadvantages, the risks and user experience and so on. Morrow B et al [4] think that Bring Your Own Device (BYOD) mainly refers to a policy that some enterprises allow employees to bring their own laptops, tablets, smart phones and other mobile devices to workplace, by which they can access enterprise's internal information and use enterprise's licensed applications. Zhang Jian et al [5] and Thomson G [6] show that the rise of Bring Your Own Device (BYOD) thanks to the transformation of IT consumption, and the development process of mobile office has mainly experienced three stages: offline mobile office, online mobile office, intelligent mobile office. Yuan Hong [7] thinks that the computing power of intelligent mobile terminals has far more than the demand of business, and there begin to appear a phenomenon of extensive use of personal devices for work in enterprises. In addition, Bring Your Own Device (BYOD) is also widely used in the field of education, and has become a new education information service mode in recent years [8]. For example, Song Yanjie [9] reports a one-year study on the project of "Bring Your Own Device (BYOD) for seamless science inquiry" in a primary school in Hong Kong, and finds that the students advanced their understanding of the anatomy of fish well beyond what was available in the textbook and they developed positive attitude toward seamless science inquiry supported by their own mobile devices. Kobus Martijn B. W. [10] investigates ownership and on-campus use of laptops, tablets, and smartphones, using survey information on Dutch university students, and it appears that the current high ownership rates of mobile IT devices by no means imply students' preference or support for university Bring Your Own Device (BYOD) strategies. What's more, Qian Yuming et al [11] analyze the three demand levels of enterprise business mobility, which in order are general office demand, enterprise application mobility demand, the scene perception of mobile devices and business smoothly handover with the scene demand. Chen Fen et al [12] and Singh N [13] analyze and compare the advantages and disadvantages of Bring Your Own Device (BYOD), then forecast the future development trend of Bring Your Own Device (BYOD). Zhou Hua [14] and Miller K W [15] et al analyze the security risks of Bring Your Own Device (BYOD), which provides an important reference for the security construction of mobile office. Tokuyoshi B [16] puts forward some suggestions of implementing Bring Your Own Device to enterprises from the perspective of user experience.

As we can see from the above, at present there is little literature that research management strategies of implementing Bring Your Own Device based on mobile Internet from the perspective of business management. In view of this, this paper bases on the analysis of the driving factors of implementing Bring Your Own Device, then points out

some new problems in the process of implementing Bring Your Own Device. Further this paper proposes corresponding management strategies which can promote enterprises to implement Bring Your Own Device, so that we can provide references for enterprises to meet the arrival of the era of mobile office.

2 Driving factors of implementing BYOD under the environment of mobile internet

2.1 The rapid development of mobile Internet and mobile terminals make mobile office become reality

With the rapid development of mobile Internet, the characteristic of mobile terminals that can surf the Internet anytime and at anywhere makes it become an increasingly important part in our daily life. According to statistics shown by the Ministry of China, by December 2015 the traffic of accessing mobile Internet up to 4.187 billion G and was up 103 percent year on year [17]. Along with the government and enterprises vigorously constructing "smart city" and "wireless city", public wireless network has been spread rapidly, and the proportion of Internet users who access the Internet through WiFi is as high as 91.8 percent [18]. The improvement of network environment and the rapid popularization of mobile Internet stimulate the demand for the application of mobile Internet and have shaped a new social life form. At the same time, the rapid development of mobile Internet and mobile terminals drives enterprises to implement mobile application solutions, and more and more employees want to freely choose their mobile intelligent devices to handle their work through mobile Internet. According to the survey data of Forrester, the majority of enterprises have begun to implement the plan of Bring Your Own Device, and 70 percent of enterprises will use some form of Bring Your Own Device program, and 62 percent of employees are already using smartphones to deal with their office affairs, and 56 percent of employees are using tablets to handle daily work. In the mobile Internet age, enterprises need more rapid and effective way of communication and way of handling business to enhance their competitiveness, and comprehensively implementing Bring Your Own Device is an inevitable trend.

2.2 The employees' growing demand for mobile office prompts enterprises to implement BYOD

With the Promotion of mobile communication and mobile terminal in service quality, function design, user experience and other aspects, more and more employees want to handle their work through mobile Internet. Because some applications of intelligent terminals have simpler operation mode and superior user experience than PC, employees want to get rid of dependence on cable network and laptop by Bring Your Own Device mode. In this way, they can make full use of fragmented time to improve the utilization of time and their work efficiency. For employees, they sometimes need to handle some business on the way to and from work; for managers, they need to look, read and review internal documents on business trip. In addition, many employees need track the progress of project, submit collected information to the internal system timely, solve users' question in the first time. So they need mobile office to help them free from the constraints of space and time, then easily deal with urgent business in hand at anytime and anyplace. The products about mobile office will not only help enterprises to implement Bring Your Own Device program to meet employee's demands for mobile office, but also will make enterprises get more business opportunities.

2.3 Mobile office mode is becoming new competitiveness of enterprise

The emergence of mobile office bring enterprise office to another new level, and enterprises' demand for information is increasingly strong. It has become an important target for enterprises to improve the core competitiveness by mobile office. According to 2016 mobile office panorama report given by the Mobile Information Research Center, mobile office is developing at an explosive speed, and more than 93 percent of CIO indicates recognition of mobility, and the number of enterprises without planning in 1-3 years falls sharply from 82.8 percent in 2013 to 6.2 percent in 2015, and the enterprises that have already deployed or being deployed are more than 40 percent. Mobile office has become an important strategic plan of enterprises. The innovation of mobile office mode makes enterprises greatly accelerate the process of enterprise mobile informationization, which leads to the improvement of the executive power and competitiveness of enterprises. Mobile office is an assistant for managers and a platform for work and communication. With the aid of mobile office, managers can timely release business notices to let employees understand enterprise culture information. At the same time, employees can submit application to managers through the mobile office system to obtain timely approval, which makes enterprises' work efficiency improved greatly. In addition, the application of mobile office, breaking the limitation of geographical space and organization, makes office action integrated. With the fierce of market competition, mobile office has become a wise choice for enterprises to enhance the core competitiveness.

3 Problems in implementation of BYOD faced by enterprises

3.1 Enterprise's application data information faces the risk of leakage

In the process of implementing Bring Your Own Device program, the influx of a large number of mobile devices has increased the amount of terminals that access enterprise. Portability of the mobile terminal and the randomness of accessing data information make enterprises' confidential data faces the risk of leakage. In general office environment, enterprises' data exist in the form of electronic documents, flowing in the office terminals and office applications, then the storage and transmission of the data are faced with different threats. The realization of mobile management of electronic documents is based on wireless network information transmission and cable network information transmission. In the office environment where information transmission entirely depends on network, no matter enterprise choose which kind of information transmission mode, the network always has many unsafe factors. In the mobile office system which involves information exchange and complex personnel communication, handling electronic documents often need information interaction. Because some electronic documents are confidential, it makes electronic documents information faces various risks brought by open network, such as computer Trojan, the invasion of virus, illegal users stealing and tampering with electronic documents, and so on. As a result, although Bring Your Own Device brings convenience to employees for work, it increases security risks of enterprise data information leakage.

3.2 The management and control boundary of mobile devices between enterprise and employees is not clear

Mobile terminal is an open platform, which can be installed software to meet the heterogenous needs of different users and be combined with related enterprise applications for mobile office. The first feature of Bring Your Own Devices is that employees can use their own mobile terminal. In relevant legal category, the definition of ownership states a fact that employees have absolute ownership and control of the devices. But in the sense where employees can use their own mobile terminal, the mobile device is a compromise between employees and enterprises. In terms of control, employees need to accept the control policy made by enterprises for security, such as strict entry authorization, device safety controls. Even enterprises and employees have reached a contract, but the devices belong to employees, so employees can control the devices as they like. Thus enterprises still need to resort to their control and management in a reasonable range. In addition, employees' personal information and enterprises' business information are mixed in the same device, while employees' main concern is their personal privacy data, so relevant monitor and management are needed in an appropriate range. This way can not only guarantee that enterprise's confidential information will not leak, but also ensure the security of user's personal privacy data. However, in the process of implementing Bring Your Own Devices program, the above mentioned management control boundary of mobile devices is not clear and most enterprises don't make strict and clear provisions in this aspect.

3.3 The employees' acceptability for BYOD is inconsistent

With the popularity of mobile Internet, more and more employees choose using Bring Your Own Device to work, but the popularity doesn't reach as high as we thought. In daily work, some employees don't use mobile intelligent terminals, such as older employees, most of them are used to the mobile devices easy to be operated, and they can not accept intelligent mobile office as fast as young people. Although mobile office is more convenient, the comprehensiveness and easy operation of desktop office system can not be denied, which is another reason why some employees can not accept Bring Your Own Device. Moreover, there exists a problem that employees' acceptability for Bring Your Own Device is inconsistent, which give rise to many difficulties when making related policies of Bring Your Own Device and implementing Bring Your Own Device, such as the scope of the executor is difficult to delineate, and employees' work is hard to perfect docking in the process of mobile officing. Therefore, while considering implementing Bring Your Own Device strategy, it should be thought carefully about employees' specific ideas and needs for mobile office. Then according to the enterprise's nature and employees' specific work, to gradually generating enterprise mobility strategies can promote mobile office and improve employees' work efficiency, which can become a new competitiveness of enterprises.

4 Management strategies of enterprises to implement BYOD

As shown in Figure 1, aiming at problems in implementation of Bring Your Own Devices faced by enterprises, next we will propose the corresponding management strategies of Bring Your Own Device in order to provide references for enterprises to meet the need of mobile office.

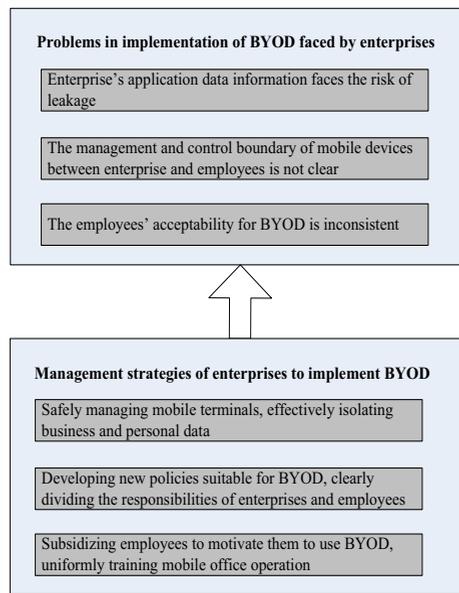


Fig. 1. Management strategies of Bring Your Own Device.

4.1 Safely managing mobile terminals, effectively isolating business and personal data

On the one hand, as a basis for judging terminals' current security state, IT management department should check whether terminals are installed anti-virus software and whether the anti-virus software is updated. And the policies which are used to ensure data security and make up for security vulnerabilities caused by employee's weak security consciousness, should include configuring and checking screen saver, checking the file sharing, checking account security and so on. On the other hand, enterprises should have full control of enterprise data information and can uniformly send the policies to each client through the BYOD server. Before the use of BYOD software, employees need to sign a confidentiality agreement to comply with the corporate policy and protect corporate data. Enterprises must ensure their data in mobile terminals have no risk to be leaked in the process of storing and transmitting. And for secure storage the data should be isolated in the sandbox. Enterprise data and applications have been isolated in the "security sandbox", and important documents and data are automatically encrypted. In this way the contents that users read and edit within the sandbox can not be copied to the outside, but also the outside data can not be copied into the sandbox. From the perspective of enterprises, this method not only ensures the safety of enterprise data, but also prevents the illegal business information (such as news, entertainment information), virus, Trojan and other illegal procedure from spreading and infecting the inner-enterprise. From the perspective of users, their personal data have been isolated outside of the "security sandbox", so they don't have to worry their personal data will flow into the enterprise Intranets and lead to the disclosure of personal privacy.

4.2 Developing new policies suitable for BYOD, clearly dividing the responsibilities of enterprises and employees

Before implementing Bring Your Own Devices strategy, enterprises should make clear, concise and strict rules for employees who use their own devices for work. Everyone who participates in the BYOD program has to sign the terms of use, and violators will not be allowed to use their own devices for work. Besides, enterprises and users should sign a privacy treaty, in which users can know what data BYOD software may involve, and obligations that enterprises and users need to follow. BYOD software should be able to allow users to decide whether the information in their terminals can be collected by the server, including GPS location, personal information and so on. In addition, it should be able to implement remote policy configuration management for mobile devices participating in the Bring Your Own Devices strategy, and the policies should be strictly divided into the policies that enterprises must follow and the policies that users can select. Users and managers could manage mobile terminals by the BYOD's server side, but their management authorities should not be the same due to their different types of job. The policies designed for managers are used for all mobile devices involved in BYOD, and the application range of these policies includes operating system types, roaming ways, encryption, the complexity of password settings and so on. Among the policies designed for users, the first are privacy policies, which includes GPS positioning, whether personal information needs to be checked, etc.. Followed by some service functions, such as remote locking, sending text messages to the terminal, removing password,

clearing information and so on. When users act against these policies, it should promptly notify managers to warn the violator and record violations, and the BYOD function of serious violator should be disabled directly and relevant data should be cleared.

4.3 Subsidizing employees to motivate them to use BYOD, uniformly training mobile office operation

When employees bring their own devices to handle office business, there should have certain requirements for mobile devices, for example, it had better to choose reputable brand mobile terminals that carry intelligent operating system. But not all employees' mobile devices meet the above requirements, thus if enterprises want to implement Bring Your Own Device comprehensively, it will certainly increase employees' average purchase costs of mobile devices and extra Internet fees in the process of mobile officing. If condition permits, enterprises should give corresponding subsidies to employees according to their actual demand for mobile office to motivate them to bring their own devices. For example, the job nature of salesman determine that their demand for mobile office is large, then enterprises can bulky purchase and configure mobile office devices; for general demand for mobile office, such as managers who release notices and employees who submit application to manager to obtain approval timely through the flow system, enterprises can give employees appropriate Internet access subsidies. Except that, enterprises can also link employees' work performance with their subsidies, then develop a reasonable and scientific distribution system of subsidies to encourage the work passion of employees. In addition, there is part of employees who are not familiar with mobile office operation, then enterprises should set up a special training course to teach them how to operate relevant mobile office system, and make them adapt to the new office mode as soon as possible. Meanwhile it will make employees carry out cooperative work more smoothly in the process of mobile officing and facilitate unified management of enterprises.

5 Conclusion

Compared with traditional PC office mode, mobile office mode has significant change and innovation. Enterprises which adopt Bring Your Own Device program not only improve the satisfaction and work efficiency of employees, but also strengthen internal information communication and information exchange with external. With the rapid development of mobile Internet and mobile terminal, as well as the ERP software vendors do further researches and make breakthroughs in enterprise-class mobile applications, Bring Your Own Device will certainly be implemented by more enterprises, which will not only make enterprises experience more convenient and efficient office mode but also enhance enterprises' competitiveness.

Acknowledge

The authors acknowledge funding from the National Science and Technology supporting Program of China (grant number No. 2015BAF05B01), as well as the contributions from all partners of the mentioned project.

References

1. S. H. Lee, B. H. Chang. *Int J Mob Commun*, **3**, 11(2013), 279-298
2. G Wu, S. Talwar, K. Johnsson , et al. *Commun Mag*, **49**, 4(2011), 36-43
3. CISCO reports: the number of mobile users will reach 5.5 billion in 2020. <http://network.chinabyte.com/279/13690279.shtml>
4. B. Morrow, *Net. Sec*, **12**(2012), 5-8
5. J. Zhang, X. Liu, *HLJ Sci Technol Info*, (2013), 99
6. G. Thomson, *Net Sec*, **2**(2012), 5-8
7. H. Yuan, *Chin New Technol New Prod*, **22**, 1(2013), 22
8. L.Y. Li, Y.L. Zheng, *Mod Dist Educ Res*, **6**(2012), 71-76
9. Y. Song, *Comput & Edu*, **74**(2014), 50-60
10. M.B.W. Kobus, P Rietveld, JN.Van Ommeren, *Comput & Edu*, **68**(2013), 29-41
11. Y.M. Qian, Z.J. Dong, D Lu, W Wang, *ZTE Technol*, **6**(2013), 33-38+42
12. F. Chen, Z.W. Zheng, *FJ Comput*, **9**(2013), 95-96+111
13. N. Singh, *J. Bus Manage & Soc Sci Rea*, **3**, 1(2012), 1-12
14. H. Zhou, X.B. Zhang, L.L. Yang, W.M. Yang, J.H. Long, *Silicon Vally*, **22**(2014), 142-145
15. K.W. Miller, J.M. Voas, G.F. Hurlburt, *IT Prof*, **14**, 5(2012), 53-55
16. B. Tokuyoshi, *Net Sec*, **4**(2013), 12-13

17. Ministry of industry and information, Economic operation of the communications industry in December 2015. 2016.01.21
18. China Internet Network Information Center. The thirty-seventh statistical report on the development of China Internet Network. 2016.01.2